



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

OPNAVINST 5530.14C CH-2
N09N3
Ser N09N3/1U533926
1 MAY 2001

OPNAV INSTRUCTION 5530.14C CHANGE TRANSMITTAL 2

From: Chief of Naval Operations
To: All Ships and Stations (less Marine Corps field
addressees not having Navy personnel attached)

Subj: NAVY PHYSICAL SECURITY

Encl: Revised pages iii, 3-1, 3-5, 4-3, 5-1 through 5-2, I-1,
I-2, VI-5 and new pages 3-5a, 4-3a, 5-2a, I-3, VI-6 and VI-7

1. Purpose. To institute within Department of Navy changes in
standoff, installation access control and waterfront security
policy.

2. Action. Remove pages iii, 3-1, 3-5, 4-3, 5-1 through 5-2,
I-1, I-2, I-3, VI-5 and replace with enclosure (1) of this
change transmittal.

David L. Brant
By direction

Distribution:
SNDL Parts 1 and 2

-	<u>PART TWO: SECURITY OF AIRCRAFT, SHIPS IN PORT PORT, AND OTHER WEAPONS SYSTEMS AND PLATFORMS ASHORE</u>	<u>PAGE</u>
0306	- General	3-3
0307	- Policy	3-3
0308	- Aircraft Security Planning	3-3
0309	- Transient or Deployed Aircraft	3-4
0310	- Other Situations	3-4
0311	- Emergency Situations	3-5
0312	- Standoff	3-5
0313	- Harbor Surveillance and Waterside/ Waterway Security	3-5a
-	<u>PART THREE: PROTECTION OF BULK PETROLEUM PRODUCTS</u>	
0314	- General	3-7
0315	- Policy	3-7
0316	- Security Planning and Liaison	3-7
0317	- Physical Security Inspections	3-7
-	<u>PART FOUR: SECURITY OF COMMUNICATIONS SYSTEMS</u>	
0318	- General	3-8
0319	- Policy	3-8
0320	- Responsibilities	3-9
0321	- Mobile Communications Systems	3-10
-	<u>PART FIVE: SECURITY OF MATERIAL</u>	
0322	- General	3-11
0323	- Policy	3-11
0324	- Responsibilities	3-11
0325	- Controlled Substance Inventory	3-12

May 1, 2001

CHAPTER 3

PART ONEPHYSICAL SECURITY MEASURES0300. SECURITY MEASURES

a. Physical security measures are necessary to establish or maintain an adequate command physical security posture. Where appropriate and feasible, physical security measures are to be coordinated and integrated on a regional basis.

b. Physical security measures are a combination of active or passive systems, devices, and security personnel used to protect a security interest from possible threats. These measures include:

- (1) Security forces and owner or user personnel.
- (2) Military working dogs.
- (3) Physical barriers, facility hardening and active delay or denial systems.
- (4) Secure locking systems, containers, and vaults.
- (5) Intrusion detection systems.
- (6) Assessment or surveillance systems (i.e., closed-circuit television or thermal imagers).
- (7) Protective lighting.
- (8) Badging systems, access control devices, material or asset tagging systems, and contraband detection equipment.

0301. ANTITERRORISM AND FORCE PROTECTION MEASURES.

Antiterrorism and force protection standards and measures are addressed in references (g) through (j).

0302. SECURITY OF FUNDS. Unless more specific measures are prescribed by other authorities, funds including cash and readily negotiable instruments will be protected in a manner that is clearly appropriate for the amount of money involved. Commanding officers shall not send armed money escorts off base without approval from the local authorities and/or the [regional commander](#).

0303. LOSS REPORTING. [Requirements and guidelines for reporting loss of arms, ammunition and explosives are outlined in reference \(e\).](#)

refueling capability for worldwide American interests. Many of these aircraft, because of their large size or mission tasking, are an attractive target. This is particularly true at installations where their presence is unusual, they are on display, or are located at civilian or foreign airfields. Refer to the security requirements matrix (table 3-1) to determine the minimum security to be provided for nonalert aircraft. These requirements apply to aircraft on display or located at civilian or foreign airfields. Special or increased requirements for specific operational configuration must be identified in advance (when possible) to host security forces.

b. Security forces in support of aircraft must be notified before a visit to the aircraft is allowed to take place. Any change in security priorities based on operational status must be identified to the host installation.

c. The aircraft commander determines if security is adequate.

0311. EMERGENCY SITUATIONS

a. Initial security for aircraft that crash or are forced to land outside a military installation is the responsibility of the nearest military installation. The owning Service will respond and assume on-site security as soon as possible.

b. In the above emergency situations, security must:

- (1) Ensure the safety of civilian sightseers.
- (2) Prevent tampering with or pilfering from the aircraft.
- (3) Preserve the accident scene for later investigation.
- (4) Protect classified cargo and aircraft components.

0312. STANDOFF

a. The standoff zone, also referred to as the setback area, is the second tier of defense and includes that space between the outer perimeter of the site and the exterior of what you are protecting. Standoff zones provide time delays and more importantly, abatement of blast effects.

b. To mitigate the effectiveness of a vehicle bomb attack, commanders shall be continually vigilant against allowing vehicle parking near high density buildings and on piers. Every attempt should be made to establish minimum standoff distances, which vary depending on the type of construction, level of protection desired and proximity of perimeter barriers. It is important to understand that explosive effects decay with

increased distance. The following are recommended minimum distances:

(1) Structural:

- 80 feet during THREATCON ALPHA*
- 100 feet during THREATCON BRAVO
- 400 feet during THREATCONs CHARLIE and DELTA

All new construction, facility modifications and MILCON projects shall comply with paragraphs 0120, 0121 and 0122 of this manual as well as the Deputy Under Secretary of Defense for Installations, Interim DoD Antiterrorism/Force Protection Construction Standards of 16 Dec 99.

* Unless otherwise hardened in compliance with DoD standards cited above.

(2) Pierside:

- 50 feet during THREATCON NORMAL
- 100 feet during THREATCONs ALPHA and BRAVO
- 400 feet during THREATCONs CHARLIE and DELTA

Every effort should be made to achieve 100 foot CONUS and 400 foot OCONUS standoff as written in OPNAVINST 3300.55 'NAVY COMBATING TERRORISM PROGRAM STANDARDS'. Distances are only applicable when an asset is present at pier.

(3) Waterside:

- 100 feet during THREATCON NORMAL
- 200 feet during THREATCONs ALPHA and BRAVO
- 400 feet during THREATCONs CHARLIE and DELTA

The above waterside standoff distances represent the outboard dimension of the innermost zone. Achievable standoff may vary based on existing structures, proximity of navigable waterways and/or as allowed by host nation agreements.

0313. HARBOR SURVEILLANCE AND WATERSIDE/WATERWAY SECURITY.
Commanding officers will ensure waterways adjacent to afloat assets are under appropriate surveillance, and where possible and as the threat dictates, or as otherwise directed, adequately patrolled.

0404. SECURITY FORCE ORDERS. The commanding officer of each installation or activity will publish and maintain security force orders pertaining to each fixed and mobile post. These orders are the written and approved authority of the commanding officer for members of the security force to execute and enforce regulations. The concept of security force orders is as follows:

a. All security force orders will specify the limits of the post, the hours the post is to be manned and the special orders, duties, uniform, arms and equipment prescribed for members of the security force. Additionally, all orders will contain guidance in the use of force, as outlined in reference (1).

b. All security force orders will be brief, concise, specific and current. They shall be written in clear and simple language. Security force orders will be under constant review and updated as required. Manpower/funding constraints mandate continuing efficient use of available security force personnel. This makes it appropriate for the security officer to conduct a total detailed review of all security force orders at least semiannually.

c. Security force orders for military and civilian guards and police will be approved and signed by the commanding officer.

0405. ARMING

a. Authority to Arm Security Force Personnel. The authority to arm security force personnel is vested in the commanding officer by reference (1), or, in overseas locations, as governed by Status of Forces Agreements. In the exercise of this authority, commanding officers will comply with requirements in reference (1). Commanding Officer's afloat will determine when to arm ship's personnel. Once the determination is made to arm, weapons will be carried loaded as required by reference (m).

b. Navy military and civilian personnel regularly engaged in law enforcement or security duties shall be armed.

(1) Personnel assigned to ship, submarines and aviation squadrons standing watch onboard, pierside or on a flightline as a collateral duty are not generally considered as regularly engaged in law enforcement or security duty.

(2) No person will be armed unless currently qualified in the use of assigned weapons. In order to qualify, Navy military and civilian personnel performing physical security/law enforcement functions must satisfactorily complete the firearms training outlined in reference (m).

(3) NO CONTRACT GUARD WILL BEAR FIREARMS ON BOARD A NAVY INSTALLATION OR ACTIVITY UNTIL WRITTEN CERTIFICATION OF

May 1, 2001

QUALIFICATION MEETING NAVY STANDARDS (reference (m) pertains) IS PROVIDED BY THE CONTRACTOR, AND THE GUARD HAS SUCCESSFULLY COMPLETED TRAINING IN THE USE OF FORCE RULES OF ENGAGEMENT. In addition, contractors must comply with provisions prescribed by the state in which the contract is administered, including current licensing and permit requirements.

CHAPTER 5

INSTALLATION ACCESS AND CIRCULATION CONTROL

0500. GENERAL

a. A system of personnel and vehicle movement control is a required basic security measure at Navy installations and activities. The degree of control must be in keeping with the sensitivity, classification, value or operational importance of the area. Visitor control relative to classified information will be in compliance with reference (a). Procedures will be coordinated among activities in the same geographical region when appropriate and feasible.

b. This chapter prescribes general policies for controlling entry into and exit from Navy installations. Access control is an integral part of the installation physical security program. Each installation or separate activity commanding officer must clearly define the access control measures (tailored to local conditions, e.g., Navy training "campuses") required to safeguard facilities and ensure accomplishment of the mission.

c. This chapter also prescribes policies for establishment of restricted areas whether by host installations, tenant activities, or by separate activities.

0501. POLICY. It is DoD policy that procedures to control access to installations and separate activities shall be developed, established, and maintained, including the following:

a. Using a defense-in-depth concept to provide graduated levels of protection from installation perimeter to critical assets.

b. Establish positive access control measures at entry control points to installations.

c. Determining the degree of control required over personnel and equipment entering or leaving the installation.

d. Prescribing procedures for inspecting persons, their property and vehicles at entry and exit points of installations or at designated secure areas within an installation, and while on the installation.

(1) This shall include determination of whether inspections are randomly conducted or mandatory for all.

(2) All procedures shall be reviewed for legal sufficiency by the appropriate general counsel or legal advisor to the Navy installation/activity prior to issuance.

e. Enforcing the removal of, or denying access to, persons who are a threat to order, security, and the discipline of the installation.

f. Designating restricted areas to safeguard property or material for which the commander is responsible.

g. Using randomized antiterrorism measures within existing security operations to reduce patterns, change schedules and visibly enhance the security profile of an installation. This reduces the effectiveness of preoperational surveillance by hostile elements.

0502. INSTALLATION ACCESS. Installation/activity commanding officers shall:

a. In addition to required armed guards, determine additional security controls of perimeter gates, i.e., barriers, video surveillance, explosives detection, vehicle inspection capabilities, etc. This determination should be based upon the results of the review and assessment processes discussed in chapter 1 and considerations discussed in chapter 2 of this manual.

b. Allocate resources necessary to enforce the established controls. These controls will be monitored and evaluated to ensure adequate protection is maintained.

0503. ACCESS AUTHORIZATION AND CONTROL SYSTEM REQUIREMENT

a. The methods used to control personnel access at an activity will be included in written procedures in the Physical Security Plan, and will include the following:

(1) Designation of restricted areas.

(2) Description of access control methods in use.

(3) Method for establishing authorization for entering and leaving each area, as they apply to both personnel continually authorized access to the area and to visitors, including any special provisions concerning non-duty hours.

(4) Details of where, when, and how security badges will be displayed.

(5) Procedures to be followed in case of loss or damage to security badges.

(6) Procedures to recover issued security badges.

(7) Measures to deny illicit use of lost, stolen, sold, or other illegally acquired security badges.

0504. EMERGENCY PLANNING

a. Installation/activity commanding officers will plan for increasing vigilance and restricting access at installations/activities under the following situations:

APPENDIX I

REFERENCES

- (a) SECNAVINST 5510.36, Subj: Department of the Navy Information Security Program Regulation
- (b) OPNAVINST S5460.4C, Subj: Control of Special Access Programs Within the Department of the Navy (U) (NOTAL)
- (c) OPNAVINST 5239.1B, Subj: Navy Information Assurance (IA) Program
- (d) OPNAVINST C8126.1A, Subj: Navy Nuclear Weapons Security (U) (NOTAL)
- (e) OPNAVINST 5530.13B, Subj: Department of the Navy Physical Security Instruction for Conventional Arms, Ammunition, and Explosives (AA&E)
- (f) OPNAVINST 5210.16, Subj: Security of Nuclear Reactors and Special Nuclear Material
- (g) SECNAVINST 3300.2, Subj: Combatting Terrorism Program
- (h) SECNAVINST 3300.3, Subj: Combatting Terrorism Program Standards
- (i) OPNAVINST 3300.53, Subj: Navy Combatting Terrorism Program
- (j) OPNAVINST 3300.54, Subj: Protection of Navy Personnel and Activities Against Acts of Terrorism and Political Turbulence (NOTAL)
- (k) SECNAVINST 5500.34, Subj: Security of DoD Personnel at U.S. Missions Abroad
- (l) SECNAVINST 5500.29B, Subj: Use of Deadly Force and the Carrying of Firearms by Personnel of the Department of the Navy in Connection with Law Enforcement, Security Duties, and Personal Protection
- (m) OPNAVINST 3591.1C, Subj: Small Arms Training and Qualification
- (n) Cancelled
- (o) NAVMEDCOMINST 6710.9, Subj: Guidelines for Controlled Substances Inventory (NOTAL)
- (p) Naval Criminal Investigative Service/COMNAVFACENGCOM Guard Services Contract Performance Work Statement (NOTAL)

- (q) SECNAVINST 5530.4C, Subj: Naval Security Force Employment and Operations
- (r) NAVSEAINST 8370.2, Subj: Small Arms and Weapons Management Policy and Guidance Manual (NOTAL)
- (s) SECNAVINST 5511.36A, Subj: Authority of Military Commanders Under the Internal Security Act of 1950 to Issue Security Orders and Regulations for the Protection or Security of Property or Places Under Their Command
- (t) SECNAVINST 5520.3B, Subj: Criminal and Security Investigations and Related Activities Within the Department of the Navy
- (u) FEDERAL SPECIFICATION RR-F-191K/GEN, 14 May 1990, Subj: Fencing, Wire and Post Metal (and Gates, Chain-Link Fence Fabric, and Accessories) (General Specification) (NOTAL)
- (v) FEDERAL SPECIFICATION SHEET RR-F-191K/1D, 14 May 1990, Subj: Fencing, Wire and Post Metal (Chain-Link Fence Fabric) (Detail Specification) (NOTAL)
- (w) FEDERAL SPECIFICATION SHEET RR-F-191K/2D, 14 May 1990, Subj: Fencing, Wire and Post Metal (Chain-Link Fence Gates) (Detail Specification) (NOTAL)
- (x) FEDERAL SPECIFICATION SHEET RR-F-191K/3D, 14 May 1990, Subj: Fencing, Wire and Post Metal (Chain-Link Fence Posts, Top Rails, and Braces) (Detail Specification) (NOTAL)
- (y) FEDERAL SPECIFICATION SHEET RR-F-191K/4D, 14 May 1990, Subj: Fencing, Wire and Post Metal (Chain-Link Accessories) (Detail Specification) (NOTAL)
- (z) User's Guide on Protection Against Terrorist Vehicle Bombs, UG-2031-SHR, May 1998, Naval Facilities Engineering Services Center, Port Hueneme, CA (NOTAL)
- (aa) NAVFAC MIL-HDBK-1013/14, Subj: Military Handbook - Selection and Application of Vehicle Barriers (NOTAL)
- (ab) NAVFAC MIL-HDBK-1013/1A, Subj: Military Handbook - Design Guidelines for Physical Security of Facilities (NOTAL)
- (ac) DoD Security Equipment Working Group Specification 012, Prime Item Product Specification for Magnetic Stripe Credentials, 18 Feb 94 (NOTAL)

- (ad) NAVPERS 15665I, Subj: United States Navy Uniform Regulations
- (ae) OPNAVINST 5585.2B, Subj: Department of the Navy Military Working Dog (MWD) Program

(4) Although public notification of designated Limited Waterway Areas is the responsibility of the local USACE or USCG, as appropriate, installation/activity commanding officers shall ensure that the language of the associate notices convey the commanding officer's intent (e.g., that such notices explicitly ban swimmers or persons as well as boats if that is what is intended).

(5) Commanding officers shall ensure that areas designated are appropriately patrolled or observed to ensure protection of ships and operations.

3. Waterfront Security. Such areas as previously described in this appendix, as a minimum, shall be designated as a Level One restricted area(s).

a. In addition to the standards set forth for restricted area and limited waterway areas and paragraphs 0312 and 0313 of this manual, waterfront areas and facilities shall be protected as follows:

(1) Barriers shall be available to prevent direct unchallenged access onto piers, wharves, or docks when ships are moored.

(2) Vehicle access to piers, wharves, or docks shall be controlled. Parking shall be limited to essential government or vetted commercial and approved ship's company vehicles. Where parking is necessary, such parking shall be commensurate with paragraph 0312 of this manual.

(3) Security planning will address additional measures to implement increased access control during heightened THREATCONS.

(4) Appropriate security force response shall be afforded to the waterfront asset or waterfront facility as defined by this manual. Security force response personnel shall be equipped with a security communications system meeting the criteria in Chapter 10 and shall be mobile or have adequate security vehicles immediately available for emergency response situations.

(5) Specific security measures for the security of ships are provided by the security matrixes at figures VI-1 and VI-2. The security of waterfront assets matrix provides a description of the Navy asset or resource to be protected and the security measures which shall be used in the protection of these assets or resources. The water asset value/risk matrix provides staffing guidelines for patrol boat tours of waterfront areas. Security measures in figure VI-1 are intended to deal with individuals or small groups (3-4 persons) approaching by boat, surface and subsurface swimmers and possessing small arms and/or explosives.

SECURITY OF WATERFRONT ASSETS MATRIX
IN U.S. NAVY CONTROLLED PORTS

<u>PRIORITY</u> <u>HIGH)</u>	<u>ASSET</u>	<u>SECURITY MEASURES (CUMULATIVE FROM LOW TO</u>
A (HIGHEST)	SSBN	.Electronic water/waterside security system (CCTV, associated alarms, surface craft or swimmer detection, underwater detection)
B (HIGH)	Carriers Other submarines	.Establish security zone with the USCG, where possible .Use water barrier(s), where appropriate and/or practical
C (MEDIUM)	Surface Combatants Amphibious Auxiliary MSC Ships (Strategic Sealift Ship (SSS) Deployed) Prepositioned Ships (loaded) Mine Warfare Patrol Coastal	.Harbor patrol boat(s) with bullhorn, NVD, spotlight, marine flares, lethal and non-lethal weapons .Establish restricted area waterway(s); with buoys and signs. Arrange patrol boat back-up support from Harbor Ops, Coast Guard, or other (tenant boat units, small craft from ships)
D (LOW)	MSC SSS (Reduced Operational Status) Pier Facilities	.Adjacent landside security (patrols, surveillance, pier access control), no special requirement in waterways

1. This matrix reflects a building block approach. Requirements for each security level are required to have in place measures from all previous priority levels plus those listed for the priority level asset to be protected.

2. Waterborne patrols are required 24 hours per day 7 days per week. For installations with priority A assets, patrols will be continuous. For installations with priority B through D assets, patrols may be random during THREATCONs NORMAL and ALPHA. However, security patrol craft must be in the water (crew nearby) and ready to get underway immediately. Commanders/Commanding Officers will decide frequency of the random patrols until THREATCON BRAVO, when they shall become continuous.

Note - Consistent with operational readiness, every effort should be made to get ships underway during increased THREATCONs.

Figure VI-1

WATER ASSET VALUE/RISK MATRIX - STAFFING GUIDELINES

<u>ASSET PRIORITY</u>	<u>THREATCONS NORMAL/ALPHA</u>	<u>THREATCON BRAVO</u>	<u>THREATCONS CHARLIE and DELTA</u>
A	1 boat; continuous patrols	2 boats; continuous patrols	Same as BRAVO
B and C	1 boat; frequent random patrols	2 boats; 1 continuous patrol - second frequent random patrols	2 boats; continuous patrols
D	1 boat; frequent random patrols	1 boat; continuous patrols	Same as BRAVO

1. Resourcing Waterborne Security:

a. Patrol boats will be assigned to installations required to protect afloat assets. The number of patrol boats assigned and the personnel required to man them will be based on type of assets to be protected and waterfront area to be patrolled.

b. The primary mission of the waterborne patrol is to deter unauthorized entry into waterside restricted areas, to maintain perimeter surveillance and intercept intruders prior to them approaching Navy ships in port. For the purpose of calculating the number of boats required, a waterborne patrol zone will nominally be 2 nautical miles, which facilitates a five-minute response time to any asset within the zone. Additional missions may include providing escorts to vessels in and out of the port area in coordination with USCG or patrolling waterfront restricted areas where ships are not present, and will be separately validated.

c. Each base with home ported waterborne assets listed above will be staffed at a minimum to support one full time security boat crew and will have at least two operational security boats to support the force protection mission.

d. A boat crew will consist of two personnel, as a minimum, and be able to sustain operations 24 hours per day 7 days per week. Coxswains may be unarmed non-security personnel, however, it is preferred that the entire crew be armed, trained security personnel.

e. Crew calculation:

(1) One boat: 7 days/24 hours (plus ½ hour extra each shift change) = 178.5 hours. Times 2 personnel = 357 hours or 11 people.

(2) Two boats: 7 days/24 hrs (plus ½ hour each shift change) = 178.5 hrs. Times 4 personnel = 714 hours or 23 people.

Note: Where practical and where the threat necessitates extended use of more than one boat, Auxiliary Security Force (ASF), where available, and/or other trained base personnel may be used to augment regular security personnel.

Figure VI-2